

Název práce: Kvantová kryptografie  
Autor: Josef Stráský  
Katedra (ústav): Katedra chemické fyziky a optiky  
Vedoucí bakalářské práce: Prof. RNDr. Lubomír Skála, DrSc.  
E-mail vedoucího: skala@karlov.mff.cuni.cz

Abstrakt: V této práci shrnuji nejdůležitější současné poznatky z rychle se rozvíjejícího oboru kvantové kryptografie. Po teoretickém úvodu, který je soustředěn na Bellovu nerovnici a důkaz neložality, jsou podrobně vysvětleny základní principy kvantové kryptografie. Kvantovou kryptografii lze rozdělit na kryptografii jedno-fotonových pulsů a na kryptografii entanglovaných stavů. Pro oba tyto typy jsou popsány hlavní způsoby kódování (polarizační a fázové) a způsoby přípravy potřebných fotonových stavů. Pro různá kvantově kryptografická schémata jsou popsány reprezentativní realizované experimenty. Přes větší technickou náročnost se ukazují výhody entanglovaných stavů. Neintuitivní vlastnosti těchto stavů vedou k procesům, které v budoucnosti umožní vznik kvantových sítí, které budou sloužit k tajné komunikaci.

Klíčová slova: kvantová kryptografie, qubit, propletenost (entanglement)

Title: Quantum cryptography  
Author: Josef Stráský  
Department: Department of Chemical Physics and Optics  
Supervisor: Prof. RNDr. Lubomír Skála, DrSc.  
Supervisor's e-mail address: skala@karlov.mff.cuni.cz

Abstract: In this work I summarize the most important knowledge in fast-developing field of quantum cryptography. After theoretical introduction, that focuses on Bell's inequation and proof of nonlocality, basic principles of quantum cryptography are explained. Quantum cryptography can be divided into the cryptography of single-photon pulses and the cryptography of entangled states. Two main methods of coding (polarisation and phase) are described for both cryptography types as well as sources of desired photon states. Important experimental realizations are described for different quantum cryptographic schemes. Despite more technical complications, entangled states indicates more advantages. Counterintuitive properties of entangled states lead to processes that allow in future formation of quantum network that will serve for secret communication.

Keywords: quantum cryptography, qubit, entanglement